SUMMARY TABLE FOR: Internet Public Key Infrastructure Caching the Online Certificate Status Protocol April 1998

24 June 1998

Prepared by:

Center for Standards
Defense Information Systems Agency

This supercedes version dated DD MMM YYYY and all earlier versions.

This Page left intentionally blank.

Disclaimer

Persons and organizations use this document at their own risk.

This document is for information only. If there is any conflict between this document and the source document, the source document takes precedence.

The U. S. Federal Government does NOT provide any guarantee as to the accuracy of this document. This document is NOT a request for proposal, a request for bid, or a modification to any contract currently held with the U. S. Federal Government.

Distribution of this document is unlimited.

Acronyms

This Page left intentionally blank.

STATUS CODES: M – MANDATORY, O – OPTIONAL, C - CONDITIONAL

SECTION	FEATURE	STATUS	REMARKS
6	**Cached OCSP Overview**		
6.1	**OCSP Entities**	M	
	Clients	M	entities which request a certificate's status
	Servers	M	entities which cache status information and respond to clients' requests
	CAs	M	entities with authoritative information about the status of some certificates
6.1.1	OCSP Clients	M	OCSP clients request certificate status information from OCSP servers.
	An OCSP client MAY be another OCSP server or CA	O	
	An OCSP client MAY be an "end" entity: one that originates a status request.	O	
	Any client MAY cache a response	O	
	Clients that are not themselves OCSP servers SHOULD use only a few, usually one, OCSP server.	O	Recommended
	Clients MUST obtain a server's key in a trusted fashion as it would the key of a trusted root CA	M	
	Clients MAY accept in-band revocation notification of a server's key	O	
	Clients MUST NOT accept an in-band replacement for a revoked server key	M	
	When a client is made aware of the revocation of a server's key, whether through in-band or out-of-band notification, it MUST NOT use that server for OCSP processing until it obtains a new key for the server via an out-of-band channel.	M	
6.1.2	**OCSP Servers**	M	OCSP servers reply to OCSP requests.
	In creating a response, an OCSP server MAY use cached information if it is appropriate	O	
	In creating a response, an OCSP server MAY forward the requests to other OCSP servers	O	
	When an OCSP server receives a query, it first checks its local store of certificate information to see if it can fulfill the request with cached data.	M	
	If the OCSP server can fulfill the request from its local store, it does so.	M	
	Otherwise, the server MAY make one or more queries to other OCSP servers that it trusts.	O	
	If it receives a definitive response from those queries (as opposed to a "status unknown" or error response), it SHOULD store that information in its local cache before returning the response to the client.	O	Recommended

SECTION	FEATURE	STATUS	REMARKS
6.1.3	OCSP CAs	M	All OCSP CAs are also OCSP servers and act in an identical fashion except that there is no need for an OCSP CA to "cache" the status of its own certificates.
	Any CA that supports cached OCSP MUST operate an OCSP server, and that server is said to be "co-located" with that CA.	M	
	A single OCSP server MAY be co-located with more than one CA.	O	
	Authoritative certificate information consists simply of the certificate and its status.	M	
	The certificate's directory entry MAY have a status attribute	O	
	The certificate's status MAY be defined by how the certificate is stored in the directory	O	
	Status MAY be determine by some other means	O	
	A co-located OCSP server MUST have direct and immediate access to a CA's internal certificate status information.	M	
	The co-located OCSP server MUST NOT receive that information via a CRL or some other periodic means.	M	
	A server that is not co-located with a CA MAY receive status information from that CA periodically	O	
7	**OCSP Caching**	M	
	A relying party MUST always be able to override any intermediary caches between it and the CA, so that it MAY (at its discretion) obtain the most up-to-date status information possible.	M	
	A relying party MUST always be given enough information to determine if a given certificate status value is acceptable for its purpose.	M	
	OCSP clients are provided with the amount of time that has elapsed since the status value was generated by the CA.	M	
	A CA MUST always be able to specify how the status for a particular certificate should be cached.	M	
	OCSP CAs MAY include recommended caching parameters in their replies that other COSP entities SHOULD observe	O	
7.1	**Correctness of Cache Entries**	M	An OCSP cache entry is said to be correct when an OCSP server can use the entry to reply to a request.
	It is "fresh enough" (see Section 7.2.2). By default, this means that it meets the caching requirements of the client, the server and the CA.	M	
	It includes a warning if the cache requirements of the client or the CA are not met.	M	

SECTION	FEATURE	STATUS	REMARKS
	If an OCSP server receives a response that it would normally forward to a client, and that response is no longer fresh, the server should forward the response to the client without attaching any warnings.	O	Recommended
	An OCSP SHOULD NOT attempt to revalidate a response that became stale in transit, as this might lead to an infinite loop.	O	Recommended
	Whenever, an OCSP server returns a response that is not "fresh enough" it MUST attach an appropriate warning to the response (see Section 8.3).	M	
7.2	**Age Calculations**	M	
	A cache entry's current age MUST be compared to its freshness lifetime (the age at which it becomes stale).	M	
7.2.1	**Current Age**	M	
	now: the current local time of the entity performing the age calculation.	M	
	producedAt: This value is the time at which the response was generated by the CA.	M	
	CAs MAY include this value in their responses.	O	
	When a response is generated from a CRL, the value of producedAt SHOULD be the value of thisUpdate field of the CRL.	O	Recommended
	requested_time: This is the receiving entity's local time when it sent the request that triggered this response.	M	
	received_time: This is the receiving entity's local time when it received the response.	M	
	age_value: This is the value of the age field in the response. This is the current age of the response as calculated by the entity sending the response at the time of transmission.	M	
	All entities MUST include an age value in any response.	M	
	OCSP ages are expressed in seconds.	M	
	Current Age Calculation	M	
	apparent_age = max (0, received_time – producedAt)	M	
	received_age = max (apparent_age, age_value)	M	
	entry_creation_age = received_age + (received_time – requested_time)	M	
	entry_local_age = now – received_time	M	
	current_age = entry_creation_age + entry_local_age	M	
	If the response does not include a producedAt value, then the received_age SHOULD be set to age_value and the first two steps above SHOULD be skipped.	O	Recommended
	When an OCSP server sends a response to any entity, it MUST calculate its current_age and include it as the value of the age field in the response.	M	
	CAs SHOULD provide an age value of 0 in their responses.	O	Recommended
	If there is a significant difference between the clocks of the calculating entity and the CA, this calculation may lead to inordinately old age values. For this reason, entities MAY ignore the producedAt value in a response and proceed as if it were not present.	O	

SECTION	FEATURE	STATUS	REMARKS
7.2.2	**Freshness Calculation**	M	The freshness lifetime of a cache entry is defined by the maxAge value specified by the CA in its authoritative response to a request.
	If this value is not present in the response, the calculating entity MAY use a locally-defined heuristic to determine the entry's freshness lifetime.	O	
	Once a freshness lifetime is obtained, the freshness of an entry is calculated by simply comparing its freshness lifetime to its current_age:	M	
	entry_is_fresh = (freshness_lifetime > current_age)	M	
7.2.3	**Disambiguating Multiple Responses**	M	
	A client MAY send out more than one request message to determine the status of a single certificate (e.g. a query MAY be sent to serveral OCSP servers). Thus, an entity may receive responses from multiple paths.	O	
	To disambiguate these responses, the client SHOULD use the one with the lowest age value.	O	Recommended
7.3	**Server Cache Management**	M	Servers are at liberty to manage their caches in any way they see fir. This section merely presents some recommendations that they MAY wish to adopt.
	When a server recovers from a crash or is restarted after being down for some reason, it SHOULD erase its cache.	O	Recommended
	If a server elects to keep its cache data between downtimes, it MUST at least ensure that the current ages of all the entries are appropriately adjusted for the missing time.	M	
	Servers MAY elect to refresh their caches periodically	O	
7.4	**OCSP Cache Entry Validation**	M	When an OCSP query includes a status value for the identified certificate (see Section 8.2), the query is called a "validation".
	Only CAs may reply to validations.	M	
	CAs MUST only reply to validations of certificates for which they are authoritative	M	
	A CA. and other servers, MAY still relay the validation to another CA or server, and return their response.	O	
	OCSP servers MUST NOT use cached data to reply to a validation.	M	
	A CA MAY reply to a validation with a normal response, or it MAY follow the procedure described in this section.	O	
	The client includes its current notion of the certificate's status in the query. Servers relay the query to the certificate's CA. When the CA receives this message, it compares the presented status with the certificate's actual current status.	O	

SECTION	FEATURE	STATUS	REMARKS
	If the statuses match, then the CA MAY return a response consisting of the certID and a responseStatus field with the value "unchanged" (see Section 8.1). The CA may include any optional fields or extensions in the response.	O	
	If the statuses do not match (i.e. the status and/or time values are different), then the CA MUST respond to the query as if it were a normal query. The CA MUST ignore the presumedStatus value presented in the validation query (see Section 8.2).	M	
	An entity that receives a responseStatus value of "unchanged" in response to a validation may recalculate the current age of its cache entry for the response's certificate.	O	
	It MUST do so by setting received_age equal to the response's age value in the response and skipping the first two steps of the calculation described in Section 7.2.1. If a server is configured to perform the this recalculation, and it is going to forward the response of the validation to a client, then it MUST perform the recalculation before realying the response. That is, the age value of the relayed response MUST be set to the newly calculated current_age.	M	
8	**Caching Enhancements to OCSP**	M	
8.1	**The unchanged Certificate Status Value**	M	
	A new certificate status is defined for cached OCSP: unchanged.	M	
	OCSPResponseStatus ::= ENUMERATED {	M	
	successful (0),	M	Response has valid confirmations
	malformedRequest (1),	M	Illegal confirmation request
	internalError (2),	M	Internal error in issuer
	tryLater (3),	M	Try again later
	notFound (4),	M	Certificate not on record
	certRequired (5),	M	Must supply certificate
	unchanged (6) }	M	Status has not changed
	The unchanged state is used in response to an OCSP cache entry validation (see Section 7.4). A CA MUST NOT use this state in response to a normal query.	M	
	When responding to a validation, a CA MAY use this state if the current state of the certificate being validated matches the presumed state sent in the validation.	O	
8.2	**The Presumed Status Extension**	O	This extension is used to create validation queries.
	A query that includes this extension MAY be treated as a validation query.	O	
	Responses MUST NOT contain this extension.	M	
	It contains the client's current notion of the certificate's status.	M	
	presumedStatus EXTENSION ::= {	M	
	SYNTAX PresumedStatusSyntax	M	
	IDENTIFIED BY id-ocsp-presumedStatus }	M	

SECTION	FEATURE	STATUS	REMARKS
	PresumedStatusSyntax ::=OCSPResponseStatus	M	
	id-ocsp-presumedStatus OBJECT IDENTIFIER ::= TBA	M	
	OCSP clients MUST NOT use the “unchanged” status value in a validation query	M	
	CAs which receive a query with this extension MAY treat the query as a validation (see Section 7.4), unless the extension value is set to “unchanged”.	O	
	In that case the CA MUST NOT treat the query as a validation. Note that queries which include an “unchanged” value in this extension do not conform to the cached OCSP protocol.	M	
	This extension SHALL NOT be marked critical.	M	
8.3	**The Cache Warnings Extension**	O	This extension contains warnings about the cache status of a certificate status response.
	This extension SHALL NOT be marked critical.	M	
	cacheWarnings EXTENSION ::= {	M	
	SYNTAX CacheWarningsSyntax	M	
	IDENTIFIED BY id-ocsp-cacheWarnings }	M	
	cacheWarningsSyntax ::= SEQUENCE SIZE (1..MAX) of SingleCacheWarning	M	
	SingleCacheWarning ::= SEQUENCE {	M	
	warning CacheWarningValue,	M	
	text UTF8String OPTIONAL,	O	
	warningData OCTET STRING OPTIONAL }	O	
	CacheWarningValue ::= INTEGER {	M	
	stale (0),	M	
	revalidationFailed (1),	M	
	disconnectedOperation (2) }	M	
	id-ocsp-cacheWarnings OBJECT IDENTIFIER ::= TBA	M	
	Each warning is assigned a number.	M	
	Each warning MAY include an explanatory text and/or some additional data	O	
	Responses MAY include more than one warning	O	
	Some warnings MUST be preserved by OCSP servers. That is, when an OCSP server receives a response that contains such a warning, it MUST pass that warning along when it relays the response,whether directly or from its cache, to a client. Warnings that must be preserved are identified in their definitions below.	M	
	stale (0)	M	
	OCSP servers MUST include this warning whenever they return a response using stale cached data.	M	
	A server MAY add this warning to any response.	O	
	A server MUST NOT remove this warning until the response is known to be fresh.	M	
	Servers MUST preserve this warning.	M	
	revalidationFailed (1)	M	
	OCSP servers MUST include this warning if they return a stale response because attempts to revalidate failed.	M	

SECTION	FEATURE	STATUS	REMARKS
	A server MAY add this warning to any response.	O	
	A server MUST NOT remove this warning until the response is successfully revalidated.	M	
	Servers MUST preserve this warning.	M	
	disconnectedOperation (2)	M	
	OCSP servers SHOULD include this warning in all responses if the server is aware that it is not connected to the rest of the network.	O	Recommended
	A server MAY conclude that it is not connected after a number of network operations fail, or it MAY be told it is not connected by an administrator.	O	
	Servers MUST preserve this warning.	M	
	An OCSP server MUST include this warning when it can not reply to anoCache query with authoritative data (either from its own store or from another OCSP server).	M	Description of noCache parameter is Section 8.5
8.4	Cache Status Information Extension	O	This extension contains information about the age of the status data in the response.
	This extension consists of 2 fields:	M	
	age: This is the age, in seconds, of the response when it was sent by an OCSP server.	M	See Section 7.2.1 for details on how the age value is otherwise calculated.
	All OCSP servers MUST include a value for age in all of their responses.	M	
	When a co-located OCSP server responds to a request about a certificate for which it is authoritative, it MUST include an age value of 0 in the response.	M	
	producedAt: This is the local time when the authoritative CA generated the response.	M	
	Only OCSP servers that are co-located with a CA MAY include this value in a response.	O	
	An OCSP server MUST NOT create this value in a response for a certificate for which it is not authoritative.	M	
	An OCSP server that receives and caches a response containing aproducedAt value MUST NOT modify or remove it when the response is used to reply to queries.	M	
	This extension SHALL NOT be marked critical.	M	
	cacheStatusInfo EXTENSION ::= {	M	
	SYNTAX CacheStatusInfoSyntax	M	
	IDENTIFIED BY id-ocsp-cacheStatusInfo }	M	
	CacheStatusInfoSyntax ::= SEQUENCE {	M	
	age INTEGER,	M	
	producedAt GeneralTime OPTIONAL	O	
	id-ocsp-cacheStatusInfo OBJECT IDENTIFIER ::= TBA	M	

SECTION	FEATURE	STATUS	REMARKS
8.5	The Request Cache Parameters Extension	O	The request cache parameters extension allows the client to specify required cache characteristics for the response.
	noCache: the client requests that the response be retrieved from the CA, i.e. that any intermediary OCSP servers ignore their caches when replying to this request.	O	
	a server that receives a request with the noCache parameter MUST NOT reply with cached data.	M	
	The server MUST either reply with authoritative information, or it MUST forward the request, including the noCache parameter, to another OCSP server.	M	
	If a server is unable to do either, then it MUST reply with a status value of unknown accompanied by a "disconnected operation" warning.	M	
	maxAge: The client requests that the response can come from a cache provided it is no older than maxAge seconds	O	See Section 7.2 for a description of cache entry age calculations.
	If a server receives a request that specifies a maxAge of 0 then it MUST attempt to validate its entry (see Section 7.4), or retrieve a fresh response from another OCSP server or, if appropriate, from its authoritative store.	M	
	Only if those attempts are unsuccessful MAY a server return a cached response older than the specified maxAge.	O	
	In doing so the server MUST include a staleness warning with the response (see Section 8.3).	M	
	minFresh	O	
	The server MAY return a cached response as long as that response is at least minFresh seconds away from becoming stale.	O	See Section 7.2 for a definition of stale.
	maxStale	O	
	The server MAY return a cached response as long as no more than maxStale seconds have elapsed since the response became stale.	O	See Section 7.2 for a definition of stale.
	noValidate	O	
	The client will accept a stale response from the server. That is, the server MAY return a stale cache entry without first validating it.	O	
	Note that any stale response MUST always include an appropriate warning (see Section 8.3).	M	
	The maxAge parameter MAY be combined with either the minFresh or the maxStale parameters.	O	
	When a server receives a request containing either combination, it MUST reply with a cached entry only if that entry satisfies both parameters, or all attempts to retrieve a satisfactory response from other servers are unsuccessful (in which case the server MUST include a warning in the response).	M	
	The noCache parameter MUST NOT be combined with any other parameter.	M	

SECTION	FEATURE	STATUS	REMARKS
	The noValidate flag MAY accompany any other parameter (except noCache).	O	
	This extension SHALL NOT be marked critical.	M	
	requestCacheParameters EXTENSION ::= {	M	
	SYNTAX RequestCacheParametersSyntax	M	
	IDENTIFIED BY id-ocsp-requestCacheParameters }	M	
	RequestCacheParametersSyntax ::= SEQUENCE {	M	
	noCache BOOLEAN OPTIONAL,	O	
	maxAge INTEGER OPTIONAL,	O	
	minFresh INTEGER OPTIONAL,	O	
	maxStale INTEGER OPTIONAL,	O	
	noValidate BOOLEAN OPTIONAL }	O	
	id-ocsp-requestCacheParameters OBJECT IDENTIFIER ::= TBA	M	
8.6	The Response Cache Parameters Extension	O	This extension allows a CA to specify required caching characteristics for the response.
	The CA MAY specify how the client's cache (if any) should handle the response.	O	
	A server that receives a response containing this extension MUST NOT remove or alter the extension when sending replies based on that response.	M	
	The server MUST preserve this extension in the same way that some warnings must be preserved (see Section 8.3).	M	
	Response cache parameters are defined by the following fields:	M	
	noCache: The receiver MUST NOT cache the response at all.	M	
	maxAge	M	See Section 7.2.2 for a description of how this field is used in cache entry freshness calculations.
	The receiver MAY cache the response	O	
	The receiver MUST consider the response stale once the cached entry's current age exceeds maxAge.	M	
	Responses with a maxAge of 0 MUST be revalidated every time they are used.	M	
	Implementations MUST NOT generate responses that include both noCache and maxAge. The ASN.1 code for this extension precludes this.	M	
	This extension SHALL NOT be marked critical.	M	
	responseCacheParameters EXTENSION ::= {	M	
	SYNTAX ResponseCacheParametersSyntax	M	
	IDENTIFIED BY id-ocsp-responseCacheParameters}	M	
	ResponseCacheParametersSyntax ::= CHOICE {	M	
	noCache [0] BOOLEAN,	M	
	maxAge [1] INTEGER }	M	
	id-ocsp-responseCacheParameters OBJECT IDENTIFIER ::= TBA	M	
9	HTTP and OCSP Caching	M	

SECTION	FEATURE	STATUS	REMARKS
	When OCSP is transported over HTTP 1.1 or higher, the caching parameters of the OCSP messages SHALL take precedence over any Cache-control directives in the HTTP messages.	M	
	When an implementation wishes to use HTTP Cache-control directives when transmitting OCSP messages, it SHOULD ensure that corresponding HTTP directives and OCSP cache parameters have the same value.	O	Recommended
	HTTP cache-control parameters MUST NOT be used as a replacement for OCSP caching parameters.	M	
	This profile recommends that HTTP caching SHOULD NOT be used for OCSP.	O	Recommended
	When an OCSP message is sent via HTTP, the HTTP no-cache directive SHOULD be used.	O	Recommended
	Although a properly-functioning HTTP 1.1 proxy MAY be employed as an OCSP cache, implementations MUST NOT assume that an HTTP proxy they're dealing with is functioning properly.	O	
	At a minimum, if use of an HTTP proxy is unavoidable then that proxy MUST at least recognize and obey the no-cache directive.	M	
10	Security Considerations	M	
	OCSP clients may require servers to contact other servers (or CAs) to respond to a request. In the event that such contact is impossible, the server MAY reply with cached information even though the client would consider such a response to be stale.	O	
	When the server responds with data it knows would not be acceptable to a client, the server MUST include one or more of the warnings described in Section 8.3.	M	
14	Appendix – Collected ASN.1	M	
	OCSPResponseStatus ::= ENUMERATED {	M	New OCSPResponseStatus definition
	successful (0),	M	Response has valid confirmations
	malformedRequest (1),	M	Illegal confirmation request
	internalError (2),	M	Internal error in issuer
	tryLater (3),	M	Try again later
	notFound (4),	M	Certificate not on record
	certRequired (5),	M	Must supply certificate
	unchanged (6) }	M	Status has not changed
	presumedStatus EXTENSION ::= {	M	Presumed Status extension
	SYNTAX PresumedStatusSyntax	M	
	IDENTIFIED BY id-ocsp-presumedStatus }	M	
	PresumedStatusSyntax ::=OCSPResponseStatus	M	
	cacheWarnings EXTENSION ::= {	M	Cache Warnings extension
	SYNTAX CacheWarningSyntax	M	
	IDENTIFIED BY id-ocsp-cacheWarnings }	M	
	CacheWarningsSyntax::= SEQUENCE SIZE (1..MAX) of SingleCacheWarning	M	

SECTION	FEATURE	STATUS	REMARKS
	SingleCacheWarning ::= SEQUENCE {	M	
	warning CacheWarningValue,	M	
	text UTF8String OPTIONAL,	O	
	warningData OCTET STRING OPTIONAL }	O	
	CacheWarningValue ::= INTEGER {	M	
	stale (0),	M	
	revalidationFailed (1),	M	
	cacheStatusInfo extension ::= {	M	Cache Status Info extension
	SYNTAX CacheStatusInfoSyntax	M	
	IDENTIFIED BY id-ocsp-cacheStatusInfo }	M	
	CacheStatusInfoSyntax ::= SEQUENCE {	M	
	age INTEGER,	M	
	producedAt GeneralTime OPTIONAL }	O	
	requestCacheParameters EXTENSION ::= {	M	
	SYNTAX RequestCacheParametersSyntax	M	
	IDENTIFIED BY id-ocsp-requestCacheParameters }	M	
	RequestCacheParametersSyntax ::= SEQUENCE {	M	
	noCache BOOLEAN OPTIONAL,	O	
	maxAge INTEGER OPTIONAL,	O	
	minFresh INTEGER OPTIONAL,	O	
	maxStale INTEGER OPTIONAL,	O	
	noValidate BOOLEAN OPTIONAL }	O	
	responseCacheParameters EXTENSION ::= {	M	Response Cache Parameters extension
	SYNTAX ResponseCacheParametersSyntax	M	
	IDENTIFIED BY id-ocsp-responseCacheParameters}	M	
	ResponseCacheParametersSyntax ::= CHOICE {	M	
	noCache [0] BOOLEAN,	M	
	maxAge [1] INTEGER }	M	
	id-ocsp-presumedStatus OBJECT IDENTIFIER ::= TBA	M	Collected OIDs
	id-ocsp-cacheWarnings OBJECT IDENTIFIER ::= TBA	M	
	id-ocsp-cacheStatusInfo OBJECT IDENTIFIER ::= TBA	M	
	id-ocsp-requestCacheParameters OBJECT IDENTIFIER ::= TBA	M	
	id-ocsp-responseCacheParameters OBJECT IDENTIFIER ::= TBA	M	

Document Point of Contact:

Defense Information Systems Agency
ATTN: JIEO-JEBBC (Gregor D. Scott)
Ft. Monmouth, NJ 07703-5613
USA
Voice: 732-427-6856
Fax: 732-532-0853
Email: scottg@ftm.disa.mil